AEDC Customer Requirements
for Using AEDC Computers & Internet Access

With the exception of the Visit Authorization Letter (VAL) which is accomplished by your Security Department and should be sent to ATA Industrial Security (Fax # (931)-454-3474 or DSN 340-3474), this document contains all the requirements for gaining access to AEDC Computers and Internet.

1. Information Assurance Awareness Program (IAAP) training
2. Virus and Incident Checklist
3. AEDC Customer Information Assurance Briefing
4. U.S. Visitor/Customer *Request to Connect Company-Owned* Personal Electronic Device (PED) to AEDC Computer Systems/Networks & Internet Access
5. Customer Information and Compliance Signature Page

USAF Information Assurance Awareness 2007 Training

1. **Objectives**:
   Focus on enhancing your awareness of threats and vulnerabilities to information systems, and to encourage the use of improved computer security practices.

2. **Why Information Assurance?**
   As size and price came down, microprocessors began to appear in the workplace, in homes, and eventually on the battlefield. What was once a collection of separate information systems is now best understood as a single, globally connected network. Because of this global connectivity, a risk accepted by one is a risk shared by all.

   Increased Risk: The exponential use of the Internet, coupled with frequent hardware and software changes, has posed a significant risk to our information. As the need for computer security increased to deal with those risks, the need to educate you on those risks has also increased. Although your role in securing information has not technically changed, the environment where information resides is constantly changing.

   Computer Security (COMPUSEC): Measures and controls that ensure confidentiality, integrity, and availability of information systems (IS) assets including hardware, software, firmware, and information being processed, stored, and communicated.

   Information Assurance (IA): Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

   A secure information system provides 5 properties:

   - **Confidentiality:** ensures people who don't have the appropriate clearance, access level, and "need to know", do not access the information.
   - **Integrity:** ensures information has not been modified during transmission or processing.
   - **Availability:** means information services are there when you need them.
   - **Non-repudiation:** ensures the sender of data is provided proof of delivery and the recipient is assured of the sender's identity so that neither can deny having processed the data.
   - **Authentication:** is a security message designed to establish the validity of a transmission, message, or originator, or a means of

verifying an individual's authorization to receive specific categories of information.

The following Information Assurance (IA) and network personnel can help you resolve IA issues and ensure the protection and defense of information and information systems.

- **Client Support Administrator: (CSA)** The CSA is the first line of help you should contact to resolve problems. CSAs possess developed knowledge of hardware, software, and communications principles, and install, configure, and operate client/server devices. They resolve the day-to-day administrative and technical system problems you experience and contact the Help Desk if they cannot resolve a problem.
- **Help Desk:** The base's focal point for problem resolution and is the primary point of contact for problems CSAs cannot resolve.

Introduction to INFOCON: The DoD INFOCON system is a series of prescribed and standardized actions to maintain or reestablish the confidence-level of networks under a commander's authority. This new INFOCON strategy shifts from a "threat-based" reactive system to a "readiness-based" proactive approach. The INFOCON system now mirrors the Defense Condition (DEFCON) system consisting of five posture levels (5, 4, 3, 2, and 1).

Your INFOCON Role: You are a vital part of the success of the INFOCON system. You may need to take actions necessary to protect DoD information systems and networks.

INFOCONs and Other Alert Systems: The INFOCON system does interact with other alert systems like the Force Protection Condition (FPCON) and Defense Conditions (DEFCON) when the situation warrants. However, a FPCON or DEFCON change does not always prompt a corresponding INFOCON level change, and vice versa.

The INFOCON system is characterized by 5 defensive postures designed to reduce risk to DoD information systems and networks.
For each INFOCON level your CSA or supporting Network Control Center (NCC) will provide you with the necessary education and awareness on threats, new vulnerabilities, and any actions you must take.

- **INFOCON 5**
  - Information networks are operational
  - Normal readiness of information systems and networks that can be sustained indefinitely
  - Impact to end-users is LOW.
- **INFOCON 4**
  - Limited risk to ongoing military operations
  - Operational impact of degradation or loss of information and information systems is LOW to MEDIUM
  - Impact to end-users is negligible.
- **INFOCON 3**
  - Risk to mission accomplishment is moderate
  - Requires vigilance to maintain network security
  - Impact to end-users is minor
- **INFOCON 2**
  - Risk of mission failure is HIGH
  - Operational impact of degradation or loss of information and information systems is MEDIUM to HIGH
  - Impact to end-users could be significant for short periods, which can be mitigated through training and scheduling.
- **INFOCON 1**
  - Risk to mission operations is EXTREME
  - Operational impact of degradation or loss of information and information systems is HIGH
  - Impact to end-users could be significant for short periods, which can be mitigated through training and scheduling.

IA policies and procedures were put in place to ensure our information systems comply with all applicable laws and reduce the security risk while ensuring operational continuity. Many of these policies and procedures outline your responsibilities to protect these information systems. To help you, there are several personnel in the IA chain of command. Don't hesitate to contact them regarding any IA issue you encounter.

3. Threat

This topic will provide you with information on threats and vulnerabilities to our information and information systems.

Threat: Any circumstance or event with the potential to cause harm to an information system through unauthorized access, destruction, disclosure, adverse modification of data, and/or denial of service.

Vulnerability: Vulnerability is a weakness in an information system, cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited.

THREAT + VULNERABILITY = RISK

Risk: The probability that a particular threat will adversely impact an IS by exploiting a particular vulnerability. Not all threats actually happen and not all vulnerabilities are exploited.

Types of Threats:

- **External Threat:** The external threat to information systems is both acts of nature, as typified by tornadoes and floods, and human, such as a hacker or protestor.
  - **Natural:** A natural or environmental threat is just what it sounds like; its source is either from nature or an information system's environment. Natural threats can include lightning, fires, hurricanes, tornadoes, or floods. Environmental threats can include poor building wiring or insufficient cooling for the information systems.
  - **Human:** Today's human threat is much more advanced than just a mischievous teenager trying to crack one computer at a time as an indoor sport. Tools available on the Internet give anyone with an agenda the capability of running automated attacks against thousands of computers at a time to identify security weaknesses. The following are a few examples of human threats: Criminal, Hacker or Cracker, Terrorist, Adversary Nations, and Allied or Friendly Nations, protester.
- **Internal Threat:** The internal threat to information systems can be categorized as intentional, such as a disgruntled employee, or unintentional, such as an accident or carelessness.
  - **Intentional:** An intentional threat could be a spy, hacker, corporate raider, or a disgruntled employee. What is an insider threat? An insider looks like you or me and is one of the most challenging security problems today. Since insiders have working knowledge of and access to their organization's computer resources, the potential for damage is great. Most insiders misuse or exploit weaknesses in the information system. Others, due to lack of training and awareness, can cause grave damage.
  - **Unintentional:** An unintentional threat could be accidentally spilling coffee or soda on your keyboard; downloading items from the Internet that may contain viruses and malicious logic programs; or leaving your computer unattended without using the screen saver lock or not logging off completely.
- **Insider Threat – What can I do?** Here are a few suggestions to help fight the insider threat:
  - Protect access to your information do not share your password.
  - Be aware of your surrounding and report suspicious behavior such as "shoulder surfing" or unauthorized access to sensitive or classified information.

- When in doubt, do not discuss your concerns with coworkers but contact your security manager or other authorized personnel.
- Activate the password-protected screen saver function on your computer.

Social Engineering: Also considered a **human** threat. Unauthorized personnel use this method to trick people into revealing sensitive information (personal information passwords, etc.) to compromise security. Social engineering techniques can occur by telephone, face-to-face, e-mail, or simply sifting through your trash.

- **"Phishing"** is an Internet e-mail scam that tricks user into revealing personal information to include Social Security Numbers, bank accounts numbers, and passwords. These e-mails look official and may ask users to reply with their information or point them to an official looking web site to provide their information. Once provided, the user could become a victim of credit card fraud and identify theft. You play a vital role in preventing social engineering. What can I do?
  - Never give your password to anyone for any reason, especially over the telephone or by e-mail.
  - Don't give out personal information about you or other employees (names, addresses, duty positions, phone numbers, etc.)
  - Don't respond to questions from telephone or e-mail surveys.
  - Verify the true identity of the call or e-mail and that it is genuine.
  - Never type things into the computer when someone tells you to unless you know the exact results of the command you're typing.
  - Don't give out details about any information system (dial-in phone numbers, private web site, private e-mail, etc.) unless they are valid users.
  - Never change your password to something someone suggests.

Elicitation: Another technique used to gain information is elicitation. The goal is to obtain sensitive information during the course of a normal conversation or in a piece of correspondence, like e-mail. Elicitation could even occur over long periods of time in an effort to gain your friendship and trust. The Internet has revolutionized elicitation, making it easier than ever to collect information from unwitting providers. Here are two ways you may be a victim of elicitation:

- **Unsolicited Requests:** Have you ever received an e-mail requesting potentially sensitive information about you, your coworkers or your work?

- **Internet Discussion Groups:** Have you ever participated in an Internet discussion group or message forum where potentially sensitive work-related issues are discussed?

Technical Vulnerability: Right out of the box, information systems are vulnerable because of bugs and defects in their software or hardware. Many times they are part of the operating system, but vulnerabilities could also be found in your e-mail, web browser, and other programs. If left uncorrected, these vulnerabilities could be exploited by hackers or viruses to obtain access and control of your computer.

Administrative Vulnerability: An administrative vulnerability is not the result of a design deficiency but is characterized by a poor policy, process, or procedure that created a security deficiency. A full correction of the vulnerability will occur through a change in policies, processes, or procedures.

Managing Vulnerabilities: New vulnerabilities to information systems are discovered every day. Managing and staying up-to-date with them can be quite difficult. Fortunately, the Air Force has a few processes to mitigate the impact of these vulnerabilities. These are handled through your CSA, Help Desk and NCC.

Vulnerability and Reporting: Contact your CSA to report vulnerability, whether technical or administrative, requiring immediate attention. This action may prevent the compromise of information or an information system. Ensure you protect the information in accordance with classification guidance.

Internet Security: There are security risks associated with browsing the Internet. The 6 most common risks are:

- **Cookie:** A cookie is a text file that a web server stores on your hard drive when you visit a site, and retrieves whenever you revisit that site. The most serious security problem with cookies has occurred when the cookie has "saved" unencrypted personal information, such as credit card numbers or SSN's.
- **Mobile Code:** Mobile code, such as ActiveX and Java, are scripting languages used for Internet applications.
- **Spyware:** More malicious than cookies or mobile code, Spyware is actually software that gathers information about you and your computer and then sends that information to the Internet without your knowledge. Spyware is typically found hidden in freeware and shareware programs. Once installed on your computer, the program sets about gathering information by various methods including scanning your hard drive, reading your e-mail or even capturing what you type on the keyboard.

- **Use of Home Internet Service Provider:** The use of commercial ISPs for official business is not encouraged due to the high operational risk posed by the possible collection of sensitive information.
- **OPSEC:** OPSEC training and education apply to computer use just as it does in conversations between personnel, correspondence, and telephone conversations. Contact your OPSEC Program Manager for more information.
- **Distributed Denial of Service Attacks:** Another threat in Internet security is the Distributed Denial of Service (DDoS) attack. These attacks involve bombarding a network resource, like a web server, with huge amounts of data from many different machines and locations in an effort to bring the server down and deny its availability. This means no one will be able to access the information residing on the server.

4. Malicious Logic

This topic will provide you with information on malicious code, how it spreads across information systems, virus prevention and what to do when a virus infects your information system.

Malicious Code: Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. Malicious Code comes in several forms to include:

- **Trojan Horse:** Hidden computer viruses or viruses in disguise. Trojan Horses are often computer programs embedded in other programs or software.
- **Worms:** A worm is an independent program that spreads copies of itself, usually through a network or other communication device. Although they don't usually modify other programs or destroy data, worms cause damage by harnessing the resources of a network, tying them up, and eventually, shutting the network down.
- **Virus:** A virus is a self-replicating, malicious code that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence.

Reasons for virus success: Viruses can invade a system through any of the normal means we use to communicate, transfer, or share data. This includes, but is not limited to, diskettes, CDs and e-mail. Their reasons for success can usually be attributed to one of the following vulnerabilities:

- Lack of awareness
- Inadequate security controls
- Bugs and loopholes in system software
- Unauthorized use
- Failing to virus scan media before introducing into an information system

How viruses spread: Viruses can spread throughout an information system in several ways:

- **Media:** Any device that can carry data can carry a virus. This includes floppy disks, CDs, DVDs, USB devices, and even music CDs. Scan any type of media with up-to-date anti-virus software before introducing it into your computer and network.
- **Web browsing:** Use caution when visiting or downloading files from web sites because viruses can attach themselves to the file, infect your computer, and spread to the entire network causing havoc on the system. This applies to sound and video files as well. If possible, download files to removable media and virus-check them before placing them on the computer's hard drive. To prevent the possibility of rapidly spreading a virus, never download files to a network or shared drive.
- **E-Mail:** Perhaps more than any other method of infection, you must use caution when opening e-mail attachments. Attachments may contain malicious code that could corrupt files, erase your hard drive, launch a destructive worm, or even allow a hacker to gain access to your computer. Be especially wary of attachments that end with .exe, .com, .vbs, .bat, or .shs extensions. Don't assume an attachment is safe because you received it from a friend or coworker. Just as with files downloaded from the Internet, a good rule of thumb is to save the attachment and then scan it with current anti-virus software before opening it.

Virus prevention tips: Here are a few key tips to help you prevent virus infections:

- Use anti-virus software
- Virus scan fixed media (laptops and desktop computers) every week, at a minimum (or according to your local security policy)
- Scan removable media (diskettes, CDs, USB devices, etc.) for viruses before each use

Signs of a virus: So how do you know whether or not a virus has infected your computer? Detecting viruses is sometimes difficult but there are a few indicators of virus infection besides alert warnings from your anti-virus software.

- Slow performance
- Files disappearing inexplicably
- Constant computer error messages
- Erratic flashing
- Constant e-mail error messages

Virus Reporting: If you suspect your computer is infected with a virus or malicious logic:

- Stop using the computer so the virus doesn't spread
- Document exactly what happened
- Call your CSA immediately

This includes reporting all virus alerts generated by anti-virus software, whether you believe them to be valid or invalid.

Hoaxes and Spam: Although not considered malicious logic by definition, hoaxes and spam could potentially cause the same type of damage to information systems and networks.

- Internet **hoaxes** are e-mail messages written with one purpose in mind-to be sent to everyone you know. Some hoaxes warn of new viruses, promote moneymaking schemes, or ask users to forward the message to friends in the name of a fictitious cause. Hoaxes only serve to slow down Internet and e-mail service for computer users by clogging in boxes and networks. If you receive an e-mail like this, don't pass it on. Delete the e-mail or pass it to your CSA for action, especially if the activity continues.
- Spam is mass mailings by individuals or commercial agencies in an attempt to overwhelm local networks with thousands of simultaneous and unwanted e-mail messages. Spam e-mails have been used to trick unwary users into clicking on a link or attachment of the message and are led to a Web site where they may unwittingly provide sensitive or personal information. The following are a few tips in handling spam:
  - Don't post your e-mail address in chat rooms, message boards (forums), or publicly open web sites.
  - Don't sign up for or participate in e-mail list-servers and news groups unless in the course of your official duties along with chain of command approval..
  - By responding, you're telling the sender your E-mail address is valid and ready to receive more spam.

Malicious logic threatens our information and information systems every day. Your awareness and proactive measures play a critical role to strengthen the security of the network and enhance mission accomplishment.

5. Roles and Responsibilities

This topic defines what is expected of you as an Information System (IS) user.

Authorized and Unauthorized Activities: AF computer assets must be treated as mission critical assets. They are provided to perform official government business or for authorized uses. Some examples of computer misuse are:

- Viewing or downloading pornography
- Gambling on the Internet
- Conducting private commercial business activities or profit-making ventures
- Loading personal software
- Violating license agreements or copyright infringements
- Peer-to-peer file sharing

Here are some common sense rules to compute by when using a government information system:

- Don't snoop in other people's computer files.
- Don't modify other people's computer work without their approval.
- Don't use a computer to steal other people's personal information.
- Don't use a computer to pose as another person.
- Don't provide your personal information (credit card numbers, social security number, etc.) unless you know the request is legitimate and your information will be protected.
- Don't use or copy software that you have not purchased.
- Don't download files or programs from web sites you're not familiar with.

Privacy Issues: Keep in mind that your rights to privacy are limited when using government computer resources. When you log on to a government system, you give your consent to monitoring. Everything you do can be monitored. Use a government-owned computer for official and authorized purposes only.

Unauthorized Hardware and Software: Misuse also includes using unauthorized hardware or software which could introduce significant vulnerabilities to AF information systems. Some examples are freeware, public domain software, and shareware and are highly susceptible to malicious logic. Coordinate with your CSA before installing any software or hardware on your government information system.

You are responsible for reporting any of the unauthorized uses to your CSA. This notification is critical because an unreported activity could jeopardize the confidentiality, integrity, and availability of our mission critical ISs.

Password Requirements: UserIDs and passwords are the most common method for identification and authentication. Poorly constructed passwords leave systems vulnerable to hackers. Properly constructed passwords make it much more difficult for a hacker to access our information systems. The following 'Password Tips' are provided concerning passwords:

- Memorize your password and don't write it down.
- NEVER share your password with **ANYONE** including CSA, Help Desk personnel, or System Administrator personnel.
- Choose a password that is at least 9 characters in length, it must contain at least two lowercase letters, two uppercase letters, two numbers, and two special characters.
- Your password must not contain any personal identity, history, or environment and must not mimic previous passwords.
- Your password must not be patterns of letters on the keyboard.
- Do not use the same password on different systems.
- Passwords to classified systems must be treated at the same level of classification as the system it allows access to.

Media and Data Control: Media is the physical medium on which data has been saved. The process you must take to erase, label, and transport each will depend on the classification of the material along with established policies and procedures. Improper use and handling of media could result in the loss or compromise of sensitive or even classified information.

Media and Classified Systems Policy:

- Scan all media for viruses before use.
- Mark media accordingly that contain classified information.
- Label CD-ROMs, or their containers or sleeves.
- Store media containing sensitive data in a secure location.
- Never use media bearing a classified label in an unclassified system.
- Introducing unclassified media into a classified computer, the media becomes classified at the same classification level as the system.

Backup Your Data: You should back up all important computer files on a regular basis. Label the backups to reflect the sensitivity level of the information they contain. Prevent erasures by keeping diskettes away from magnetic sources such as radios and telephones. Store the media in areas safe from potential fire and water damage.

Data Classification Issues: Proper protection of our information is critical to information assurance. The Department of Defense has three broad categories of information: Unclassified, Sensitive, and Classified.

Data Protection: All DoD information, individually or in aggregation, warrants some level of protection. As a minimum:

- All DoD unclassified information must be reviewed before release outside the U.S. Government. This includes information on Air Force public web sites.
- Caution must be used to prevent data aggregation. This occurs when data, although unclassified, is combined with other unclassified information to possibly provide an adversary an insight into our capabilities, intentions, and limitations.

Sensitive Information: Sensitive information includes personnel, medical, operational, and financial information and usually falls under the Freedom of Information Act (FOIA) as For Official Use Only (FOUO) and Privacy Act marked material. When sending this type of information across the Internet, whether through web sites or e-mail, use an appropriate level of protection to prevent unintentional or unauthorized disclosure.

Differences between NIPRNet and SIPRNet: The Non-Secure Internet Protocol Router Network (NIPRNet) is just that: a non-secure, or unclassified, unencrypted network that does not provide a secure level of protection for information traversing it. The Secret Internet Protocol Router Network (SIPRNet) is a U.S.-only system used for transmission of classified information. It provides a level of protection for data up to and including SECRET.

6. New Developments

This topic will provide you with information on new developments in computer technology that impact Information Assurance.

New Technologies: New technology brings new vulnerabilities to our information and information systems and has the potential to endanger our Information Assurance security posture unless properly managed. As a user of these items, you must be aware of the risk involved with their operations.

- **USB Devices:** USB devices (e.g., flash, pen, and jump drives) offer the capability of massive storage coupled with the convenience of a small keychain size item. This may present both a security threat and vulnerability and you must follow established policy regarding such items to include local requirements.
- **Laptops:** The convenience of laptops also makes them vulnerable to theft or security breaches. Password-protect the logon to your laptop. Be careful what you display on your screen, especially in close quarters such as airplanes.

- **Personal Digital Assistants (PDAs)**
  PDAs pose a security threat for a number of reasons. Their small size and low cost make them easy to obtain and difficult to control. They have tremendous connectivity and storage capabilities. **NEVER** place classified information on a PDA.
- **Biometrics:** Biometrics is measurable physical characteristics or behavioral traits used to verify the identity of an individual when accessing an information system or even a secure facility.
- **Wireless:** Wireless networks and devices are easily susceptible to interference, jamming, and exploitation. Because of this, the use of wireless technology must be implemented in strict accordance with established DoD and AF policy. Do not connect wireless devices to the network without contacting your CSA.
- **Risks with Remote Access:** Webmail and Remote Access Service (RAS) allow you to access your email account and home network from a remote location. Always protect your password when using this type of system.
- **Common Access Card (CAC):** The CAC will be used in the DoD for all unclassified smart card functions. The CAC combined with your personal identification number (PIN) will allow you to access your workstation and DoD PKI protected web sites.

You must be aware of your Information Assurance responsibilities with new technology and follow the specific guidance and procedures in DoD and AF security policies. New security mechanisms are being developed to help you. These include the Public Key Infrastructure and your Common Access Card.

You play a vital role in all these area to ensure the protection and defense of our information and information systems.

7. Software Licensing and Anti-Piracy

After completing this topic, you should be able to identify the consequences of violating copyright laws

This lesson will discuss software licenses and copyright protection. The U.S. Code has specific provisions for copyright protections of software. The software developers through the licensing agreements accompanying their software execute this copyright protection.

Copyright - Protected by Law: All software products and user documentation are protected by law. The unauthorized reproduction of software is punishable by statutory damages and may result in a felony conviction. This topic covers the following information:

- **What is a Copyright?** A copyright is a form of statutory protection, which allows its owner the exclusive right to control, among other things, the copying, distribution, and preparation of derivative works

of authored materials. International treaties and laws in most countries provide for protection of software under copyright provisions. All software products, including graphics and user documentation, are protected by copyright. The rights granted to the user of software products are conveyed to the user by the software license agreement.

- **Copyright Infringement:** Software creates unique problems for copyright owners because software is so easy to duplicate and the copy is usually as good as the original. This fact, however, does not make it legal to violate the rights of the copyright owner. Software is a medium of intellectual property and its protection is grounded in the long-established copyright rules that govern other more familiar media, such as records, books, and films. The unauthorized duplication of software constitutes copyright infringement regardless of whether it is done for sale, for free distribution, or for the copier's own use. Moreover, those who copy are liable for the resulting copyright infringement whether or not they know their conduct violated Federal law.
- **License Agreements:** A software license agreement is a legal agreement in which the software developer executes powers of copyright. The license is an agreement between a software user (the licensee) and the software developer that defines the terms and conditions under which the software and its accompanying materials may be used.
- **Software Piracy:** Unauthorized reproduction of software contrary to the software publisher's End User License Agreement. Many people do not understand that you do not own the software program, but simply purchase a license that specifies how the software may be used. You are allowed to make a single copy of the program for backup purposes, but it is against the law to give copies to friends and/or colleagues.

  On 30 September 1998, the President issued Executive Order (EO) 13103, Computer Software Piracy, establishing policy for the prevention of software piracy. Each Government agency is responsible to ensure it does not procure or distribute software in violation of copyright laws and that only legal software is installed on agency computers.
- **Criminal Prosecution:** Laws and regulations throughout the world condemn software piracy. For example, in the United States, software piracy is punishable by statutory damages of up to $100,000 for each work infringed and may result in a felony conviction. Penalties for felony convictions include fines of up to $250,000 and imprisonment for up to five years!

License Agreements: Software licensing agreements come in many forms and are very specific as to how the licensed user may use the software. The following information is covered in this topic:

- **Single-user vs. Multi-user:** A single-user license permits the software to be loaded on only one computer. It does not allow a single person to use the software on multiple computers. Multi-user licensed software, such as concurrent licenses, site licenses and enterprise licenses, gives an organization considerable flexibility to negotiate agreements that make software available to multiple users operating on a network.
- **Upgrades:** A software license agreement is a legal agreement in which the software developer executes powers of copyright. The license is an agreement between a software user (the licensee) and the software developer that defines the terms and conditions under which the software and its accompanying materials may be used.
- **Academic Editions:** Academic Edition (AE) software is discounted for use in the academic arena (e.g., schools, students, teachers, or researchers). Unless you qualify for this version and buy it from an authorized reseller or the software publisher, do not purchase AE software. Consult the software publisher regarding specific eligibility qualifications.
- **Shareware:** Shareware, or "user-supported" software, is copyrighted software that the developer encourages you to copy and distribute to others. This permission is explicitly stated in the documentation or displayed on the computer screen. The developer of shareware generally asks for a registration fee if you like the software and plan to use it. By registering, you may receive further documentation, updates, and enhancements. You are also supporting future software development. NOTE: By giving you permission to copy and distribute shareware, the developer is not giving you permission to distribute it for profit.
- **Freeware:** As the name implies, this type of software is distributed freely, with no usage cost. Freeware is protected by copyright law and does have licensing agreement that need to be followed. NOTE: Just as with Shareware, by giving you permission to copy and distribute freeware, the developer is not giving you permission to distribute it for profit.
- **Public Domain:** Public-domain software authors dedicate their software to the public domain, which means the software is not subject to any copyright restrictions. It can be copied and shared freely. Software without copyright notice is usually, but not always, in the public domain. Before you copy or distribute software that is not explicitly in the public domain, check with your network administrator.
- **Air Force Guidance:** It is Air Force policy that licensed, registered software, including shareware, acquired through Government

procurement is the only commercial software authorized to be installed on Government computers. The Air Force allows the use of public domain, freeware or shareware software only after it is certified by a software testing facility and approved by the DAA.

Remember, the unauthorized duplication of copyrighted software is not legal regardless of whether it is done for sale, for free distribution or for the copier's own use, and it is punishable by fines and imprisonment.

Software licensing and anti-piracy laws and policies are important aspects of the information assurance awareness program. This lesson has provided you with the basics to aid in your understanding.

"USAF Information Assurance Awareness 2007"
Answer Sheet

Name: _____Company: _____Date: _____

1. ___
2. ___
3. ___
4. ___
5. ___
6. ___
7. ___
8. ___
9. ___
10. ___
11. ___
12. ___
13. ___
14. ___
15. ___
16. ___
17. ___
18. ___
19. ___
20. ___

21. ___

"USAF Information Assurance Awareness 2007" Unit Test

1. As the need for computer security increased to deal with new risk to our information the need to educate you on those risks has decreased.
   a. True
   b. False

2. Which of the following actions should you not take during an INFOCON to ensure the integrity of DoD information systems and networks?
   a. Reporting anomalous activity to your CSA
   b. Vigilance in computer security practices
   c. maintaining situational awareness
   d. Disregarding INFOCON information from your CSA or NCC

3. The possibility that a particular threat will adversely impact a particular vulnerability of an information system is called _____.
   a. Risk
   b. Threat
   c. Vulnerability
   d. Weakness

4. Tricking people into revealing passwords and other information to compromise the security of your information system is an example of _____.
   a. Elicitation
   b. Social Engineering
   c. System Administration
   d. Dumpster Diving

5. What type of internal threat looks like you or me and is one of the most challenging security problems today?

   a. Weakness
   b. Threat
   c. Vulnerability
   d. Insider

6. What type of software is typically found hidden in freeware and shareware programs and gathers information about you and your computer to send to the Internet?
   a. Cookie
   b. Internet Service Provider (ISP)
   c. Mobile
   d. Spyware

7. Which one of the following statements is true?
   a. By giving you permission to copy and distribute shareware, the developer is **not** giving you permission to distribute it for profit.
   b. Freeware is provided at no charge, and therefore is **not** protected by copyright law and has no licensing restrictions.
   c. When you purchase an upgrade to software you already own, you may move the old version to another computer and continue to use it.

8. It is okay to occasionally conduct personal business activities using a government computer resource as long as it doesn't interfere with your work.
   a. True
   b. False

9. What should you do if you receive an e-mail that warns about new viruses, promotes moneymaking schemes, or asks you to forward the e-mail to everyone you know in the name of a sick child?
   a. Report the e-mail to your CSA
   b. Forward the e-mail to everyone you know
   c. Delete it.

10. Which of the following are valid passwords? **Choose more than one answer**.
   a. BearsFan
   b. 7@Da15L#m
   c. 100620027
   d. pF&12Uq8@

11. Which of the following networks provides a level of protections for data up to and including SECRET?
   a. NIPRNet
   b. LAN
   c. WAN
   d. SIPRNet

12. Software or firmware capable of performing an unauthorized function on an information system designed with a malicious intent to deny, destroy, modify, or impede configuration, program, data files, or routines describes _____.
   a. Shareware
   b. Hackers
   c. Freeware
   d. Malicious Code

13. What type of attack bombards a Web server with huge amounts of data from many different machines and locations in an effort to bring the server down and deny its availability?
   a. Conventional Warfare
   b. DDoS
   c. Trojan Horse
   d. Web page defacement

14. Which of the following is not a reason for successful virus infections?
   a. Lack of awareness
   b. Anti-virus software
   c. Unauthorized use

15. Technical Sergeant Payton finds his system has detected a virus, which was sent via e-mail. What should Technical Sergeant Payton do?
   a. Send an e-mail to everyone in the unit, letting them know what he found

b. Panic
c. Destroy his computer's hard drive
d. Notify his CSA.

16. USB devices do not fall under any established policy regarding portable or removable media.
    a. True
    b. False

17. Which of the following types of software is **not** copyright protected?
    a. Freeware
    b. Shareware
    c. Public domain software
    d. Trial software

18. When you purchase an upgrade to software you already own, you may move the old version to another computer and continue to us it.
    a. True
    b. False

19. What type of threat can include poor building wiring or insufficient cooling for the information systems?
    a. Hacker
    b. Human
    c. Internal
    d. Natural or environmental

20. Biometrics uses physical characteristics to validate an individual when transmitting Data over the Internet.
    a. True
    b. False

21. Which of the following statements is true with regard to violating software copyright laws?
    a. Copyright laws are a guideline for the use of software but seldom result in criminal penalties.
    b. Violations of copyright laws may result in a fine, imprisonment, or both.
    c. As long as a user copies copyrighted software for their own personal use, there is no need to worry about software piracy laws.

ARNOLD ENGINEERING AND DEVELOPMENT CENTER
INFORMATION ASSURANCE OFFICE ARNOLD AFB

Virus & Incident Checklist

VIRUS

Contact your Information System Security Officer (ISSO) or immediate supervisor. ISSO: Contact NCC at 4040 Identify if the virus was downloaded from a document.

- ¸ Do NOT turn off your computer!
- ¸ Write down any errors that you observed on your system.
- ¸ Mark the computer "**DO NOT USE**".

INCIDENT

If classified information is accidentally placed on your system do the following IMMEDIATELY!

Notify, in person or via secure phone, your ISSO and the Help Desk at 4040.¸ Follow Help Desk instructions.

- ¸ Do not delete the message/file.
- ¸ Turn off your machine and mark it "**DO NOT USE**".
- ¸ Have someone with the appropriate clearance physically guard the machine or secure in area cleared for same classification level.

.

AEDC CUSTOMER INFORMATION ASSURANCE BRIEFING

1. Computer use at AEDC is monitored (Internet usage and sites).

2. In accordance with National Industrial Security Program Operation Manual (NISPOM) guidelines, hardware, software, and media shall be marked upon creation with the classification level clearly indicated. Also, all data with military application requires distribution statements, export control warning notices, and destruction notices, as directed by the appropriate DoD User Agency.

3. Software, media, equipment, or other materials shall not be removed from AEDC without proper authorization and instruction.

4. Passwords for computers that connect to any AEDC resource must consist of nine (9) characters (2 upper case, 2 lower case, 2 numbers and 2 special characters (@&+! etc). **Do not write passwords down.**

5. Passwords for computers that connect to any AEDC resource must be changed every sixty- (60) days.

6. **Use Password-protected** screen savers and ***immediately*** activate whenever computers are left unattended.

7. Most test environments at AEDC are located in Closed or Restricted Secure areas. Access to these areas is granted based on the appropriate clearance level and need-to-know, as specified on the test customer representative's Visit Authorization Letter (VAL), which should also identify the requirement for Automated Information Systems Equipment (AISE) access.

8. While at AEDC, area access will be monitored. Customer access is limited to the applicable testing area, if applicable and specified support areas, the cafeteria, and the credit union. **Do not** venture into other areas unless authorized by the ATA Security Office or the Air Force Project Manager.

9. The use of electronic devices (beepers, pagers, laptops, palmtops, blackberries, multi-function, calculators and organizers with non-volatile memory, cellular telephones, two-way radios, etc.) in a Closed or Restricted area is prohibited.

10. Customer-owned AISE that will be connected to AEDC computer/network resources or the Internet must have virus scanning software and be coordinated through the ATA/IA Office. AEDC procedures require Air Force approval of all AISE processing information at AEDC **prior to** the AISE becoming operational.

11. Customers wanting to connect to AEDC computer/network resources must provide verification (SSAA) of the approved processing level of any equipment brought from a non-AEDC location, to include the configuration, hardware, and software to be used. (Internet use only does not require a SSAA).

12. Customers shall ensure all processing units and software are scanned/checked for viruses **prior to** connecting to AEDC computer systems.

13. All AISE and Closed/Restricted areas are subject to inspection at any time. Customers shall follow applicable AEDC security procedures and practices so that AEDC can continue to provide an excellent security environment in support of AEDC test facilities.

U. S. Visitor/Customer *Request to Connect Company-Owned* Personal Electronic Device (PED) to AEDC Computer Systems/Networks or Internet

(This page is not required if you **are not** connecting to AEDC Computer/Network Resources or the Internet).

PEDs include company –owned laptop computers, handheld computers, personal digital assistants (PDAs), bar code readers, and cellular telephones, etc.

To avoid delays at Pass & Registration, this page must be completed and faxed (931)-454-3581 to the ATA/IA Office, ATTN: D. J. Jackson, prior to your visit.

Name of PED User:			
Type of PED:			
PED Manufacturer & Model Number:			
PED Serial Number:			
Does your laptop have wireless capability (Bluetooth, WiFi, IR)? PCs/laptops with wireless technology installed will have that capability disabled and IR ports will be covered with opaque tape prior to being used at AEDC	**Circle:**	**YES**	**NO**
Is the PED company/government owned? (Personally owned PEDs are **not** authorized for use at AEDC)			
Name of company/organization which owns the PED:			
Location where the PED computer will be used at AEDC:			
Length of time authorization is required **Start Date:** **End Date:**			
PED connectivity to any AEDC computer system or network is authorized only with additional AF approval.			
Purpose for which PED will be used?			
Is Internet access required?	**Circle:**	**YES**	**NO**
Is a Virtual Private Network (VPN) Required?	**Circle:**	**YES**	**NO**
USAF/Aerospace Testing Alliance (ATA) Point of Contact			

Complete this page and Fax to (931)-454-3581, ATTN: D.J. Jackson, if you have any questions, please call (931)-454-3871. The area this is being faxed is **not** an open area.

Customer Information and Compliance Signature

Citizenship_____

Social Security Number_____

AEDC POC/Sponsor:_____

Print Last Name: _____

Print First Name:_____

Middle Initial (if any)_____

Company Name_____

Company Address_____

Company City, State_____

Business Telephone Number: (_____)-_____

Job Title_____

E-Mail Address:_____

By signing below, I have read, understand, and agree to comply with the AEDC Information Assurance briefing as stipulated herein, and as addressed in the Information Assurance Awareness Program (IAAP) training, which I have completed, to include the examination.

Signature_____Date_____

Notice: This page contains Privacy Act Information of 1974.

"USAF Information Assurance Awareness 2007"
Answers

1. _B_
2. _D_
3. _A_
4. _B_
5. _D_
6. _D_
7. _A_
8. _B_
9. _A,C_
10. _B,D_
11. _D_
12. _D_
13. _B_
14. _B_
15. _D_
16. _B_
17. _C_
18. _B_
19. _D_
20. _A_
21. _B_